Installing Natural Security

This document describes how to install Natural Security on a mainframe computer under all mainframe operating systems and TP monitors supported by Natural using an Adabas database.

The following topics are covered:

- Prerequisites
- Installation Tape for Natural Security
- Installation Procedure
- Installation Verification
- Natural Security in a Heterogeneous Environment
- Setting Up Natural Security in a Heterogeneous Environment

Prerequisites

The following software must be installed and running before you can install Natural Security:

- Natural for batch
- TP monitor(s)

You are recommended to install Natural Security **after** all other subproducts of Natural, as this makes defining the subproducts' system libraries to Natural Security easier.

If you are using parallel versions of Natural Security it is **strongly recommended** that you always use the highest version to perform data maintenance.

mation, see Application Interfaces in the Natural Security documentation.

Additional Prerequisites for Natural Security in a Heterogeneous Environment

In addition to the prerequisites described above, the following software must be installed and running in order to use Natural Security in a heterogeneous environment:

- Entire Network version *
- Natural Security for Mainframes (IBM, BS2000, AS400) *

* Version as specified under Natural and Other Software AG Products in the current Natural Release Notes for Mainframes.

The following software must be installed as required:

- Natural Security for UNIX
- Natural Security for Windows
- Natural Security for OpenVMS Version 5.1

For further information, see Setting Up Natural Security in a Heterogeneous Environment.

Prerequisite for the Natural Development Server Part

The following is required:

- INPL of Natural Security Version 3.1.5 or above
- Enable SYSSEC to maintain Natural Development Server specific profiles.
- Add basic application profiles to the FSEC system file which are prerequisites for maintaining Natural Development Server specific profiles.

See also Application Protection, Prerequisites (in the Natural Security documentation).

Installation Tape for Natural Security

The installation tape contains the dataset NSC*nnn*.INPL (where *nnn* represents the version number of the product). This dataset contains the Natural Security modules in a format loadable with the Natural system command INPL.

For a detailed description of the installation tape refer to the **Report of Tape Creation** which accompanies the tape.

Installation Procedure

It is recommended that you install Natural Security **after** all other subproducts of Natural, as this makes defining the subproducts' system libraries to Natural Security easier.

Step 1: Create System File - Job I050, Step 9900

Only perform this step if you wish to use a new FSEC system file for Natural Security Version 3.1. If you wish to use an existing Version 2.2 or 2.3 FSEC system file, omit this step.

If you wish to have the FSEC as VSAM system file, please refer to the Natural for VSAM Interface documentation for information on how to install the FSEC system file and details concerning restrictions on the use of the FSEC VSAM system file.

Load the Natural Security system file (FSEC) using the Adabas utility ADALOD (ADALOD is described in the **Adabas Utilities Manual**). Input for ADALOD is the dataset NAT*nnn*.SYSF. The file number you specify for the FSEC system file must be as yet unused.

This step creates an empty system file for Natural Security.

Step 2: Create Log File

(Job I050, Step 9901)

This step must only be performed if the Natural Security function "Logging of Maintenance Functions" is to be used. Otherwise, omit this step.

Load the log file using the Adabas utility ADALOD (ADALOD is described in the **Adabas Utilities Manual**). Input for ADALOD is the dataset NSC*nnn*.SYSL.

This step creates a log file to be used by the above-mentioned function.

Step 3: Adjust Natural Parameter Modules

(Jobs I060, I080)

- Add the following profile parameter to all your Natural parameter modules:
  `FSEC=(,`*`file-number`*`)`
  where *file-number* represents the number of the Natural Security system file - either the new one loaded in Step 1 or the existing Version 2.2 or 2.3 one.
  (If required, you can also specify a database ID, password and cipher code with the FSEC profile parameter; refer to FSEC - Natural Security System File in the Natural Parameter Reference documentation.)

- In all your Natural parameter modules, set the profile parameter DATSIZE to a value of at least 64.

Repeat jobs I060 and I080 for all your TP monitors.

Step 4: Load Natural Security Modules

(Job I061, Step 9900)

Once this step has been performed, it is not possible to remove Natural Security from the Natural system file; to remove Natural Security from the system file again, you would have to delete the entire contents of the system file and re-install all Natural components again.

Load the Natural Security modules using the Natural system command INPL (described in the in the Natural System Command Reference documentation).

This step loads the Natural Security modules into your Natural system file (FNAT) under the library ID "SYSSEC" and the logon-processing programs under the library ID "SYSLIB".

This step also results in the creation of the following security profiles and relationships:

- A library security profile with library ID **"SYSSEC"**. The library is people-protected ("People-protected" set to "Y" and "Terminal-protected" set to "N").
- A user security profile with user ID **"DBA"**, user type ADMINISTRATOR, and password set to "DBA".
- User "DBA" is linked to library "SYSSEC" (ordinary link, no special link).

If INPL is executed again for Natural Security, the Natural Security modules will be newly loaded without affecting any objects and relationships already defined after the initial execution of INPL.

If you execute INPL with the option "RECOVER", the user "DBA", the library "SYSSEC", and the link between the two will be redefined as after the initial installation, while all other links to "SYSSEC" will be cancelled.

Step 5: Change Password of User "DBA"

Invoke Natural.

On the Natural Security logon screen, type in library ID "SYSSEC", user ID "DBA", password "DBA", and a new password, and press ENTER.

Type in the new password again and press ENTER to confirm the password change.

Step 6: Define Administrators

This step must only be performed if Version 3.1 is your first version of Natural Security; that is, if you have not used any previous version of Natural Security. Otherwise, omit this step.

Create a user security profile for each person who is to be a Natural Security administrator; and then link each Natural Security administrator to the library SYSSEC. The following is an *example* of how to do this.

- On the logon screen, type in library ID "SYSSEC", user ID "DBA" and the password as established in Step 4.
- The Natural Security Main Menu will be displayed. On this, enter code "M".
- A window will be displayed. In this window, mark object type "User" with a character or with the cursor.
- The User Maintenance selection list will be displayed. In the command line of the User Maintenance selection list, enter the command "ADD".
- A window will be displayed. Choose a user ID for your Natural Security administrator (for example, if the administrator’s name were Arthur Dent, you may choose "AD" as his user ID; the following steps will take this as an example). In the window, type in user ID "AD" and user type "A".
- The Add User screen will be displayed.
  Enter the user name "Arthur Dent" and set Private Library to "N" (and press ENTER).
- Press PF3. User Arthur Dent is now defined to Natural Security under the user ID "AD".
- The User Maintenance selection list will be displayed again. In the "Co" column of the selection list, mark user "AD" with function code "LL".
- A window will be displayed. In the window, enter library ID "SYSSEC".
- The Link User To Libraries selection list will be displayed. In the "Co" column of the selection list, mark library "SYSSEC" with function code "LK". User Arthur Dent is now linked to library SYSSEC.
- In the command line, enter the direct command "LOGOFF". The Natural Security logon screen will be displayed.

Now you can log on to SYSSEC with user ID "AD" and password "AD". When you log on with the new user ID for the first time, you must change the password (by typing in a new password in addition to the user ID and password).

Once you have successfully defined administrators, it may be advisable to delete user DBA to make sure that the user ID "DBA" cannot be used by unauthorized users to gain access to SYSSEC.

To delete user DBA:

- Log on to SYSSEC with user ID "AD".
- Go to the User Maintenance selection list as described above.
- On the list, mark user "DBA" with function code "DE".
  A window will be displayed, in which you enter and confirm user ID "DBA".
  The user DBA is now deleted.

Step 7: Define System Libraries

Only perform this step if Version 3.1 is your first version of Natural Security; that is, if you have not used any previous version of Natural Security. Otherwise, omit this step.

Create security profiles for all system libraries of Natural and Natural subproducts installed at your site; see also Adding a New Library (in the Natural Security documentation).
Refer to the installation instructions for other Software AG products for the corresponding security definitions to be performed.

To automatically create security profiles for system libraries (that is, all libraries whose IDs begin with "SYS"), proceed as follows:

- Use the function "System Libraries Definition".
- Log on to library "SYSSEC".
- On the Natural Security Main Menu, select "Administrator Services".
- On the Administrator Services Menu, select the function "System Libraries Definition".

When you invoke the function, a list of the system libraries of Natural and all Natural subproducts installed at your site will be displayed. For each system library, a library-specific security profile is provided in which all the necessary components are already defined appropriately.

On the list, you can either mark with "AD" individual libraries to which you wish their pre-defined profiles to be applied one by one,
or you can choose to have the pre-defined profiles applied to all product system libraries simultaneously by marking the corresponding product with "AD".

> **Note:**
> This step should not be performed for SYS libraries containing Natural utilities, as it is recommended that these utilities be protected as described in the section Protecting Utilities (in the Natural Security documentation).

If you use the function "System Libraries Definition"in an initial installation, you have to set the Natural profile parameter MADIO to a value of at least "2000".

Installation Verification

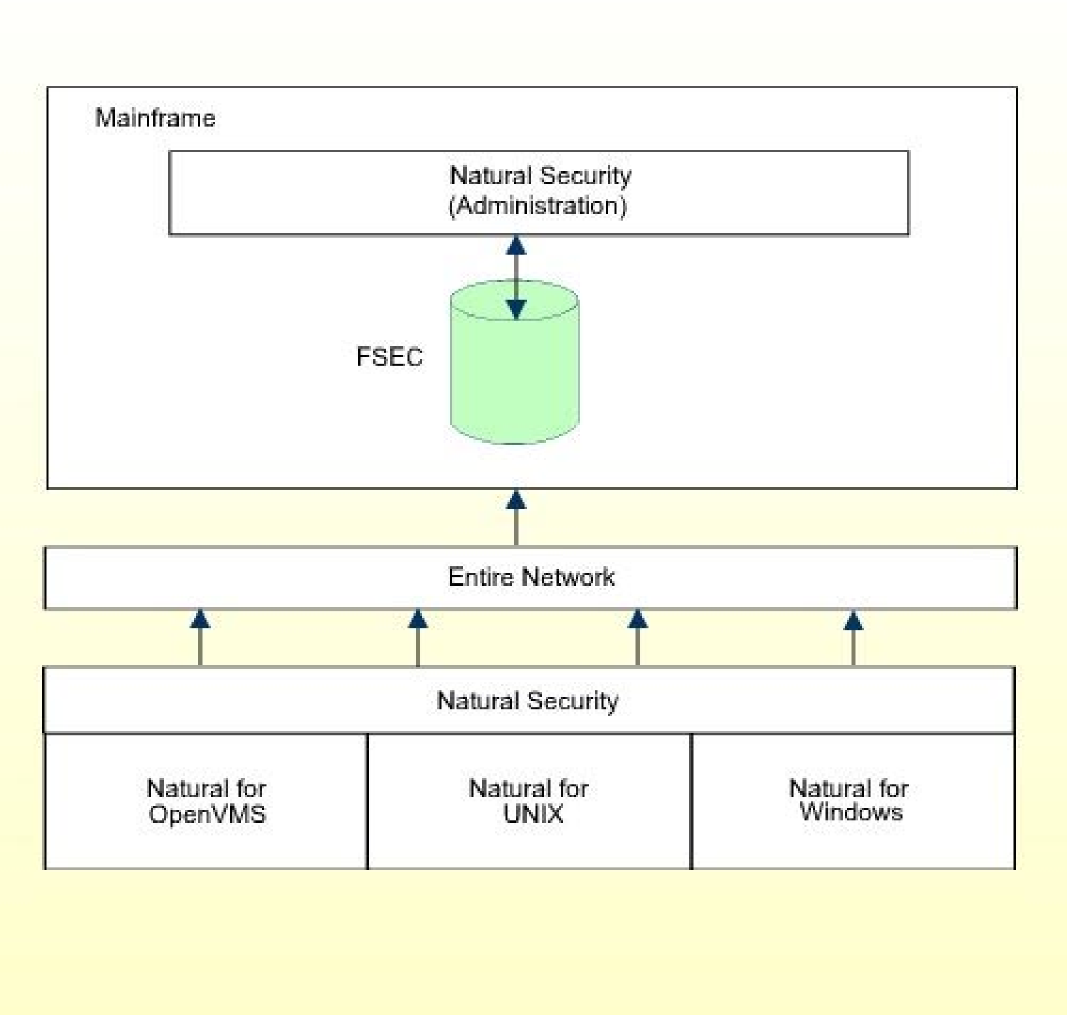
After Step 5 of the installation procedure has been completed successfully, Natural Security is operational.

Repeat the "Installation Verification" procedure for all Natural subproducts installed at your site.

Natural Security in a Heterogeneous Environment

With Natural Security Version 3.1 and above for mainframes, all enterprise security profile data can be stored and administrated centrally in a mainframe system file, which is accessible to a heterogeneous environment, thus simplifying and standardizing security maintenance on a company-wide basis. The security data in the mainframe Natural Security system file (FSEC) can be retrieved via remote database calls, managed by Entire Net-Work, from the following Natural Security installations:

- Natural for OpenVMS Version 5.1
- Natural for UNIX
- Natural for Windows



All maintenance and administration of security data is done on the mainframe installation. In the non-mainframe Natural Security installations, the security data maintenance application SYSSEC is disabled, as are the following Natural Security interface subprograms for modifying security profiles:

- NSCLI
- NSCOB
- NSCUS

If these interface subprograms are invoked, error NAT0828 is returned.

For further information on setting up Natural Security in a heterogeneous environment, see below.

Setting Up Natural Security in a Heterogeneous Environment

This section covers the following topics:

- Configuring Entire Net-Work
- Customizing the Natural I/O Conversion Table on Non-Mainframe Platforms
- Setting Up Module Access
- Setting Up Natural DDM Security

Configuring Entire Net-Work

Entire Net-Work's translation process is centered around the format and length of each field specified in the search and format buffers that are passed with each Adabas call, along with special translation definition parameters. When a request goes through the network conversion routines, each individual field is translated according to the format and length defined for it in the associated search or format buffer.

To avoid the errors NAT0824 and NAT0825, add translation definitions for the following fields for the DBID and FNR of the mainframe system file FSEC with format "X":

- LW
- LC
- LQ
- LV
- LS

This prevents values being either translated or swapped.

For further information, see the section **Special Handling of Field Format "X"** in the section **Heterogeneous Platform Considerations** in the **Entire Net-Work Installation and Operations for Mainframes** documentation.

Customizing the Natural I/O Conversion Table on Non-Mainframe Platforms

If you want to use special characters not contained in the default Natural character set (ISO08859), for example in passwords, you must customize the Natural I/O conversion table in the following sections of the file NATCONV.INI:

```
ISO8859_1->EBCDIC

EBCDIC->ISO8859_1
```

You can use the call CMCNV provided in the module SULCONV in the library SYSTRANS to check the settings.

For further information on the file NATCONV.INI, see the Installation documentation for the relevant platform.

Setting Up Module Access

When you are using Natural Security cross-platform, security profiles held in the mainframe FSEC will usually apply to data held in libraries on another platform.

If you use the Allow/Disallow Modules definition, it is recommended that you use the "Module names held in the user buffer" fields of the library maintenance function Disallow/Allow Modules screen. For modules which are not on the mainframe FUSER, use the Free List.

For further information, see the section Disallow/Allow Modules (in the Natural Security documentation, section Library Maintenance).

Setting Up Natural DDM Security

If you want to use a non-mainframe platform as your Natural development environment, you must move any DDMs required by Natural modules to the library SYSTEM (FUSER). This is necessary because Natural Security runtime only checks DDMs located in the library SYSTEM.